INFORMATION MANAGEMENT PRINCIPLES APPLIED TO THE BALLISTIC MISSILE DEFENSE SYSTEM

THESIS

John M. Koehler II, Captain, USAF

AFIT/GSS/ENV/07-M2

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GSS/ENV/07-M2

INFORMATION MANAGEMENT PRINCIPLES APPLIED TO THE BALLISTIC MISSILE DEFENSE SYSTEM

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Space Systems

John M. Koehler II, BSE

Captain, USAF

March 2007

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/GSS/ENV/07-M2

INFORMATION MANAGEMENT PRINCIPLES APPLIED TO THE BALLISTIC MISSILE DEFENSE SYSTEM

John M. Koehler II, BSE
Captain, USAF

Approved:

Alan R. Heminger (Chairman)	2 Mar 07 date
Michael R. Grimaila (Member)	02 MAR 07 date
Todd A. Peachey (Member)	2 MAR 07 date

Abstract

Information systems (IS) have evolved over the last 50 plus years from individual components with single functionality to grand architectures that integrate multiple individual business functions into global organizational enterprises. Similarly several military systems with the single mission of missile defense have evolved in service stovepipes, and are now being integrated into a national and global missile defense architecture. The Missile Defense Agency (MDA) is currently tasked with developing an integrated Ballistic Missile Defense System (BMDS) capable of defending against all ranges of ballistic missiles in all phases of flight in defense of the homeland, our deployed forces, and our allies. While this initiative has been proceeding since before Ronald Reagan's Strategic Defense Initiative, the full momentum has only recently been achieved through the withdrawal of the Anti-Ballistic Missile Treaty and demonstrated threats from North Korea and Iran. This study draws parallels between the evolution of IS and the BMDS. Further it compiles information management (IM) principles, investigates if they apply to the BMDS, and investigates if they can be used to achieve a better integrated system. Initial indications are that IM principles do apply, but it is questionable if they are being applied.

Acknowledgments

I would like to thank the members who participated in the Delphi Group. Their participation was insightful and invaluable. I would like to thank my committee for their guidance and inputs. Their help provided much needed form and structure to this amorphic idea. I especially would like to express my gratitude to my thesis advisor. Without his mentorship this thesis would have never been written. His wisdom gave me the tools to develop this idea into something worthy of being written. Finally, I thank my wife. Without her I would have never found the time or strength to get through my most academically challenging effort to date.

John M. Koehler II

Table of Contents

Page

Abstract iv

Acknowledgements v

Table of Contents vi

List of Figures viii

I. Introduction 1

General Issue 1
Background 2
Problem Statement 8
Research Questions 10

II. Literature Review 12

Evolution of Ballistic Missile Defense System Elements 12
Air Force Elements 12
Air Borne Laser 12
Space-Based Infrared System/Defense Support Program 13
Satellite Tracking and Surveillance System 15
Navy Elements 16
Aegis Ballistic Missile Defense 16
Army Elements 17
Terminal High Altitude Area Defense 17
Patriot Advanced Capability-3 18
Joint Elements 19
Command and Control, Battle Management, and Communications 19
Ground-based Midcourse Defense 20
Kinetic Energy Interceptor 22
Summary 22
Evolution of Computer Based Information Systems and Information Management 23
Parallels between Information Systems and Ballistic Missile Defense System 28
Information Management Principles 29
Information Strategy 30
Information Technology 33
Change 35
Change Management 35
Changing Information Market 36
Organizational Change 37

Page

Value 38
Alignment 39
Standards 41
Information Architecture 42
Culture 44
Information Life Cycle 46

III. Methodology 49

IV. Results and Analysis 52

Initial Delphi Results 53
Application 53
Application of Non-applied Principles 53
Non-applicability 54
Application to BMDS Integration 54
Additional Results 55
Second Round Delphi Results 57
Summary 59

V. Discussion, Conclusion, Recommendations 61

Discussion of Delphi Results 61
Conclusions 63
Limitations of Research 64
Recommendations for Future Study 64

Appendix A. Human Subjects Exemption Approval Letter 65

Bibliography 66

Vita 69

List of Figures

Figure Page

1. IM Principles Compiled from Literature Review 14

2. Initial IM Model Constructed from 9 IM Principles.....17

3. Summary of Results from Delphi Group 20

4. Modified IM Model Based on Delphi Group Results.....23

INFORMATION MANAGEMENT PRINCIPLES APPLIED TO THE BALLISTIC MISSILE DEFENSE SYSTEM

I. Introduction

General Issue

The MDA has been tasked to develop the BMDS. This system will be relied upon to protect our nation's homeland, military personnel and assets abroad, allies' homelands, and deployed personnel. Missile defense systems have been in development ever since the first V-2 rocket was launched by Germany in WWII. In 1981 Ronald Reagan gave a speech envisioning a world (not just our nation) free from the threat of ballistic missiles starting the development of a missile defense system resembling what we have today. The result of this long development is a set of legacy and new stovepipe systems developed with integration as an afterthought. While technology has provided methods to link all these systems together, technology does not offer a total system plan for the proper integration of these systems. As the BMDS was being designed, the computer revolution unfolded and with it the information age was ushered in. As this occurred the discipline of managing information progressed through missteps and mismanagement. Today IM is a mature discipline with many lessons learned in project management and creating systems of systems that deal with information. With an analogous evolution, IM should provide insight into how the BMDS could be integrated as a complex information system using IM principles.

Background

The issue of missile defense has existed since the first flight of the V-2 rocket (General Accounting Office, 1993). This event spurred a chain of events characterized by changing missile defense architectures. These architectures were influenced by the threat environment, technical possibility, and politics.

In 1955 the Army and Air Force (AF) began assessing the possibility of a BMDS. From this, the Army produced the Nike-Zeus system comprised of four radars, the Zeus missile, and a computer fire control system (General Accounting Office, 1993). The system became the first operational BMDS in 1965 (Jane's Information Group, 2005).

In 1967 President Lyndon Johnson made the Nike-Zeus our first National Missile Defense (NMD) system named Sentinel. The architecture was to cover 14 locations, 10 of which were major cities (Larsen & Kartchner, 2004). But, in 1969 President Nixon made his mark by downsizing the architecture to provide for defense of U.S. Minuteman intercontinental ballistic missiles (ICBM) at Grand Forks Air Force Base, N.D., and at Malmstrom Air Force Base, Montana, together with a Ballistic Missile Defense (BMD) Center at Cheyenne Mountain Complex, Colorado (General Accounting Office, 1993). Additionally, he changed the name to Safeguard (MDA Historian Office, 2001). One of the reasons for the shift in defense locations was political discontent about the idea of nuclear tipped missiles possibly exploding and reigning debris over the population centers the system was meant to protect (General Accounting Office, 1993).

In 1972 the Anti-Ballistic Missile Treaty was signed along with an additional protocol in 1974 that altered the Safeguard system design. The treaty limited the USSR

and USA to one site with no more than 100 interceptors (General Accounting Office, 1993). Grand Forks became the first US BMD site on 1 October, 1975. The site was only operational for four months, however, because Congress deemed it too costly to sustain (Larsen & Kartchner, 2004). The treaty also set a precedent distinguishing between theater missile defense (TMD) and NMD. This distinction set a precedent for developing systems separately for each mission and limiting their scope.

The most dramatic revolution in BMD architecture came after Ronald Reagan gave a speech envisioning a world free from the threat of ballistic missiles. This speech came after the president was informed of Russia's new ICBM capability of raining thousands of nuclear warheads down over the US (General Accounting Office, 1993). President Reagan along with Secretary of Defense Weinberger created the Strategic Defense Initiative (SDI) (General Accounting Office, 1993). Under SDI a new massive system of systems was conceived with the mission of defending against the Soviet threat (General Accounting Office, 1993). In 1987 a Phase I architecture included (MDA Historian Office, 2001):

- Space-based Interceptor (SBI)
- Ground-based Interceptor (GBI)
- Ground-based Sensor (GBS)
- 2 Space-based Sensors (SBS)
- Battle Management System

To manage this undertaking the Strategic Defense Initiative Organization (SDIO) was created with an AF General as director (General Accounting Office, 1993). The process for acquiring this system would be an evolutionary incremental development with a

phased deployment providing incremental capability. The capabilities sought would be based on arms control negotiating leverage rather than technical or threat based merit (General Accounting Office, 1993). This affected the system's development progress. A Defense Science Board criticized the SDIO citing "weaknesses in management and technical support for system design and integration" (General Accounting Office, 1993). Technology still influenced design, however. In 1989 the system exploited the miniaturization revolution in computers and sensors replacing the SBI (a large warehouse satellite that launched kill vehicles) with a system coined Brilliant Pebbles (thousands of tiny individual space-based kill vehicles) (MDA Historian Office, 2001).

Again, in 1990, world events such as the fall of the Berlin Wall led to reexamining policy and technical goals of the SDI. The SDIO initiated a new study for an architecture optimized for current threats (General Accounting Office, 1993). In 1991 President George H.W. Bush provided input to SDIO resulting in the Global Protection Against Limited Strikes (GPALS) system. This system, as its acronym suggests, was focused on limited strike scenarios such as those witnessed in Desert Storm (as apposed to massive volume of incoming warheads) (Larsen & Kartchner, 2004). The new architecture was now composed of (General Accounting Office, 1993):

- Patriot
- Corps Surface to Air Missile
- Terminal High Altitude Area Defense (THAAD)
- Brilliant Pebbles
- NMD: GBI, GBS, SBS
- Battle Management, Command, Control, Communications system (BM/C3)

GPALS only lasted until 1993 when yet another review was conducted for a new president. Under the Clinton Administration the Bottom-Up Review (BUR) was lead by Secretary of Defense Les Aspin finding that TMD was now the primary threat BMD was to defend against (General Accounting Office, 1993). This finding was partially based on intelligence community estimates and placed TMD as the priority with NMD a far second. Secretary Aspin announced the "end of the Star Wars era" and renamed SDIO the BMD Organization (BMDO) (General Accounting Office, 1993). The new system had distinct architectures for TMD and NMD. The TMD system included (Larsen & Kartchner, 2004):

- Patriot
- THAAD
- Aegis

The NMD system included (General Accounting Office, 1993):

- SBS
- GBS
- GBI
- BM/C3

Although the Grand Forks BMD system was terminated in 1976, BMDO still planned to use the site and the 100 interceptor design for initial deployment of NMD to comply with the ABM Treaty (General Accounting Office, 1993).

Despite a new architecture and new name for its lead organization, BMD maintained two trends. First, the major issue facing BMD was "integration of the various elements into a single system (General Accounting Office, 1993)." Second, and perhaps

a driver for the first trend, while a single organization was charged with overseeing the development of a BMD system, the Army, Navy, and AF all separately pursued programs (Larsen & Kartchner, 2004). To combat this integration issue, at the direction of the Under Secretary of Defense for Acquisition and Technology, the BMDO established a Joint Program Office in 1997 and awarded Boeing a contract to act as Lead System Integrator. However, this was only for the NMD system (MDA Historian Office, 2001).

The next significant era in BMD was marked by a new BMDO Director, AF Gen Ronald T. Kadish appointed in 1999 and newly elected President George W. Bush. Together, they significantly reorganized BMD. President Bush did three significant things in 2001. First, he withdrew from the ABM Treaty which released political constraints on possible systems (Hewish, 2002). Second, he attempted to combine TMD and NMD into a single architectural concept (Larsen & Kartchner, 2004). Third, he restructured the BMDO and renamed it the MDA. Raising the organization to agency status meant it could be appropriated more money signifying its political importance (Larsen & Kartchner, 2004).

On December 17, 2002 President Bush made another revolutionary move announcing intentions to deploy a missile defense with initial capability by 2004 (Larsen & Kartchner, 2004). This would be the last significant change for BMD. In the face of these radical changes, historical trends continued. The administration continued the concept of an evolving architecture that reacted to current threats and utilized emerging technologies (Larsen & Kartchner, 2004). To produce this evolving architecture, systems would be procured through spiral development in support of incremental block acquisition (Larsen & Kartchner, 2004). In 2002, Secretary of Defense Rumsfeld

announced the continuance of the TMD priority. He also described today's ambiguous overarching guiding BMD concept: a layered defense composed of systems that attack ballistic missiles of all types (short, medium, intercontinental) in all phases of flight (boost, mid-course, terminal). Finally, he announced the AF, Army, and Navy would still separately deploy elements of the BMDS (Larsen & Kartchner, 2004). There was one slight break from tradition. Instead of waiting for a complete, integrated, fully capable system, any system with any amount of initial capability would be fielded (Larsen & Kartchner, 2004). The new concept called for fielding the following systems as soon as some capability existed (Larsen & Kartchner, 2004):

- NMD located at Fort Greely, Alaska with 20 GBIs
- Aegis
- Patriot Advanced Capability-3
- THAAD
- Upgraded GBS
- SBS

This brings us to today's system which has not changed significantly since 2002. MDA continues to use an evolutionary acquisition strategy that provides added capabilities through new technologies (proven or not) in two year block increments (General Accounting Office, 2006b). The systems this strategy is producing are discussed in Chapter 2. The current threat environment includes ICBMs from North Korea and short and medium range threats from the Middle East. Political influence is motivating development to address long range threats from Iran (Sirak, 2004). Perceived capability would undoubtedly be used for negotiations with Iran with respect to Iraq.

One new development is international involvement. As the BMDS is projected globally, international partners are beginning to come on board. Australia, Japan, and the United Kingdom have all began participating in joint BMD activities (Sirak, 2004).

The history of BMD has been one of changing architectures driven by politics, the threat environment, and technology. Through the various influences, many things remained the same. The acquisition strategy has been one intended to accommodate a changing architecture capable of responding to current threats. For most of its life, the BMDS has been championed by a single organization, yet elements were pursued by separate services in isolation. Finally, the integration issue has remained the most troubling challenge consistently put off as long as possible.

Problem Statement

In June 1999 Lt Gen Ronald Kadish, Director of the BMDO stated, "Our main challenge, now that we have a plan, is to execute it with people and the resources available. I really don't see us having a huge technological mountain to climb in the sense of having to invent a lot of [new technologies]. The challenge is beginning to be more **management** than it is technical to pull this very complex set of technologies together and ... put together a layered defense." (Sirak, 2001) (emphasis added)

For more than 50 years the Department of Defense (DoD) has been pursuing a system to protect against ballistic missiles. The Navy, AF, and Army have pursued their piece of the pie in virtual isolation, despite an appointed organization with oversight of the overall system. Visions of this system have been ambiguous with the requirements

even more ambiguous. Yet, the DoD has persisted in attempting to put a system together with no concrete blueprint. Billions of dollars have been spent on the system with no defined plan of how to get from the concept to the end product. Today there are numerous systems with varying capabilities that contribute to the overall mission. The DoD continues to develop the system with no hard architecture or set of requirements. The current philosophy is to build something, test it, and evaluate the next step. This has lead to test failures, cost and schedule overrun, and unverified capability. Voicing the inadequacy of this philosophy, Gen Kadish has said the current system has a "better than zero" chance of accomplishing its primary mission; intercepting a ballistic missile (Brown, 2005). He stated that the issue is a management issue, yet only technical solutions continue to be explored. This current method is not working.

The BMDS is composed of many types of systems: weapon systems, sensors, communications systems, and computers. Combined, this system is traditionally seen as a defensive weapon system. If you look at how the system accomplishes its tasks, however, it can be seen as a large complex information system. Once a sensor detects the plume of a launched target, data is created. That data then traverses the system through a network to a computer console where it is transformed into information presented to a decision maker. The decision maker then internalizes the information, combines it with additional information and knowledge, and puts forth an order for action. Looking at the BMDS to include the people, command structure, organization and processes, it fits the model of an IS. Treating the BMDS as an IS, can IM principles be applied to provide solutions to the management problem of integrating the various elements?

Research Question

The Air Force has commonly been viewed as the technologically advanced service. Technology is viewed as the panacea for all problems. Even when management programs have been instituted such as Total Quality Management, they have devolved to mathematical solutions such as metrics. Knowledge Management has devolved to a peer to peer information depository known as Air Force Knowledge Now. Technology costs money and with the DoD's ever shrinking budget it has never been more critical to find cost effective solutions to our problems.

The discipline of IM has grown along with the evolution of computer-based information systems. Through many missteps, proven methods for managing large, complex, global IS have evolved. The aim of this evolution has focused around information and how to exploit it fully. IM may be applicable in the military to field systems better, faster, cheaper, and with better quality. There seems to be common themes in IM that apply to military systems. Themes such as Information Strategy, Information Architecture, Culture, Standards, Value, Change, Information Life Cycle, Alignment, and Information Technology could be used in implementing BMDS elements to produce a more efficient system. For instance, the theme of Standards is important. Information must be presented in a standard fashion so that anyone can understand and interpret the information presented. The BMDS is comprised of more than eight elements operated by three services and multiple nations. If information presented by the various systems is not standard, and the services do not have a standard for the information these systems present, then how can a commander or even the systems of one

service accurately and correctly interpret information from the various elements and various services?

To illustrate, assume the Air Force system defines “Boost Phase” as 0 to 80 miles, but the Army defines it as 0 to 60 miles, and these services provided the inputs for their respective systems. An AF satellite detects a launch and codes it as being in its boost phase when the target is at an altitude of 65 miles. The AF satellite sends this information to an Army Command and Control (C2) system. An Army commander then assigns an Army interceptor with a range of 0 to 60 miles to take out the target. The intercept will fail because there was not a system-wide standard for the term “Boost Phase” during system design. Applying the IM theme of standards ensures this mistake will not happen.

Comparing the evolution of IS and the BMDS reveals obvious similarities. The most striking is how each started as component technologies used to address specific singular functions. As technology evolved, these systems became more capable and able to address multiple functions. Now, each has the capability to be used in addressing large scope issues such as business administration and missile defense. IM has also evolved to manage the increasingly complex IS. As it has evolved several themes that govern the management of IS have developed. Analyzing the literature can produce a set of governing principles for IS. The research question is: Do Information Management Principles apply to the BMDS? Can they be applied to find non-technical solutions to integrating the BMDS?

II. Literature Review

Evolution of Ballistic Missile Defense System Elements

As Chapter 1 explained, the BMDS has had many different architectures composed of various elements. Today's architecture has its own unique set of components tasked with defending against various ranges of missiles in various phases of flight. These components are to be integrated and managed as a layered system. A single element is being tasked with integrating all the other elements. Some of these elements are legacy systems; they have been upgraded for missile defense. Other elements are new programs, but based on old ideas. Most of the systems have been developed in service isolation despite their joint overall missions. The following provides brief overviews of the elements' histories, programmatics, and challenges.

Air Force Elements.

Air Borne Laser (ABL).

The ABL is designed to destroy ballistic missiles in their boost phase of flight (General Accounting Office, 2006a). It is a modified Boeing 747 with a sensor/tracking system, battle management system, and laser (General Accounting Office, 2006a).

The program was started in 1996 with Boeing as the prime contractor and Lockheed Martin and Northrop Grumman (NG) as subcontractors (General Accounting Office, 2006a; Hewish, 2004). The Air Force provides primary government oversight and reports to MDA. The acquisition strategy is to develop the system in incremental, capability-based blocks (General Accounting Office, 2006a). This plan calls for bringing

a capability to attack short to medium range ballistic missiles initially, and ICBMs in the future (Larsen & Kartchner, 2004).

Since the program has started, it has been restructured (in 2004) and battled technical integration difficulties which have delayed the program passing the prototype phase until at least 2008 (General Accounting Office, 2006a). Ninety-four percent of the prototype's engineering drawings have been released, yet no BMDS integration tests have been performed (General Accounting Office, 2006a). Integrating the ABL may be difficult since it was designed to be self contained from launch detection to kill, which makes sense, since it would be unlikely to be able to respond to a threat not within its range (*BMDS booklet: A day in the life of the BMDS*2006).

Space-Based Infrared System, Defense Support Program (SBIRS/DSP).

SBIRS/DSP are AF satellites with sensor payloads that detect infrared events on Earth. These AF assets are tasked with four missions; only one of which is Missile Defense: tracking rockets from launch to terminal descent and passing on the track data to the BMDS and interceptor systems supporting MDA. SBIRS' three additional missions are: Missile Warning, detection of rocket plumes and notification to USNORTHCOM; Technical Intelligence, gathering data for rocket characterization supplied to the intelligence community; and Battle Space Awareness, gathering data on IR events on the ground to better characterize the battlefield situation in near real time in support of theater commanders (Burkett, Daniel L., II, 1998).

DSP has been around for over 30 years developed by NG for the AF with the sole purpose of detecting ICBM launches during the cold war (Burkett, Daniel L., II, 1998). In Desert Storm DSP's ability to detect Scud launches demonstrated additional capability

in theater defense. Wanting to expand on this capability and exploit the full potential of IR technology, SBIRS was conceived (Burkett, Daniel L., II, 1998).

SBIRS began development in 1995 as a replacement for DSP and to be the flagship program for Acquisition Reform (AR) (General Accounting Office, 2006a). The original constellation was to be composed of four satellites in geosynchronous orbit, two payloads on host satellites in highly elliptical orbits, a low earth orbit constellation of 20 satellites (now STSS), and ground stations (Burkett, Daniel L., II, 1998). The SBIRS contract was awarded to Lockheed Martin (LM) with the AF providing government oversight (Hewish, 2004). It was to follow a traditional acquisition strategy, but institute the latest AR initiatives such as Cost as an Independent Variable (CAIV), minimal military standards, commercial off-the-shelf (COTS) technology, and Total System Program Responsibility (TSPR) (Lorell & Grasser, 2000). In this vein the government provided a general set of requirements to LM who was supposed to use their expertise to fulfill them. However, in the course of its design, the disparate user community pressured the program managers to add specific requirements (that conflicted between communities) late in development (Crock, 2002). This was compounded by a changing threat environment that further exacerbated the requirements creep. One requirement that has been publicized is the use of a 1970's programming language (Singer, 2005). This was an example of using COTS when inappropriate since it required large modifications for the SBIRS cutting edge requirements.

These issues have resulted in technological problems such as integrating satellite systems, multiple program restructuring continually delaying delivery of the first satellite, and cost and schedule overruns (General Accounting Office, 2006a). The DoD has

become so disheartened that a new system is being conceived to replace SBIRS which has yet to launch a satellite. Since no satellite has launched, no operationally realistic tests have been accomplished to integrate the system with the BMDS or any other element.

Space Tracking and Surveillance System (STSS).

STSS was originally a component of the SBIRS architecture. It was conceived as a low earth orbiting constellation of 20 to 24 satellites with the primary mission of tracking all ballistic missiles in all phases of flight and discriminating reentry vehicles from countermeasures. It additionally carried the three other SBIRS missions as well.

In 2000 the contract for SBIRS Low was given to MDA who renamed it STSS and dropped the other three mission areas (General Accounting Office, 2006a). NG was awarded the contract for development with Raytheon as a primary subcontractor. The AF performs primary oversight and reports to MDA. STSS follows an acquisition strategy of spiral development supporting 2-year incremental block development (General Accounting Office, 2006a). This is intended to allow technologies to mature and then implement them as they are proven. In reality, various technologies are being tested on satellites acquired through traditional acquisition cycles of around 10 years. These different technologies will be tested and then the most viable technology will be incorporated in the operational system several years in the future.

Despite the restructuring of the program and a new acquisition strategy, technical problems have still been encountered integrating components from different contractors (General Accounting Office, 2006a). The STSS Block 06 satellites have not been

realistically tested for integration with the BMDS. However, the final system that would be integrated with the other elements has yet to be conceived.

Navy Elements.

Aegis Ballistic Missile Defense (BMD).

The Aegis BMD system is a complete missile defense system composed of an AN/SPY-1 radar sensor capable of tracking short and medium range ballistic missiles in all phases of flight, a fire control system linked to the BMDS network, and SM-3 interceptor missile capable of destroying short and medium range ballistic missiles in all phases of flight (General Accounting Office, 2006a). LM is the prime contractor while Raytheon is the prime developer for the SM-3 missile. The system is based on the Aegis combat system originally conceived in 1969 and has remained under the supervision of the Navy.

The Aegis BMD system has had many successes with six successful intercept tests (the most realistic) since 1999 (General Accounting Office, 2006b). One quality contributing to this success is an inherently open architecture that relatively easily accepts upgrades using COTS systems (Brown, 2005). This attribute supports the *build as you go* methodology prominent in MDA.

The Aegis combat system was originally conceived for defending against small cruise missiles and aircraft. As theater defense became a hot issue the Aegis systems were upgraded to additionally defend against short range and medium range ballistic missiles starting in 1995 (General Accounting Office, 2006a). This move was pushed by the Navy after Desert Storm and validated by the DoD in 1992 (General Accounting

Office, 1993; Larsen & Kartchner, 2004). In January of 2002 MDA recognized the system's potential and claimed several ships renaming them Aegis BMD systems (General Accounting Office, 2006a). Since then the focus has been on upgrading the system to integrate into the BMDS architecture. This is done through incremental, capability based 2-year blocks (General Accounting Office, 2006a).

While piece-meal integration tests have been performed with various BMDS elements, an end-to-end flight test with the Ground-based Missile Defense (GMD) system (with which it is conceptually supposed to support) has yet to be performed (General Accounting Office, 2006a). Nevertheless, on 24 September, 2004 the USS Curtis Wilbur deployed to Japan for the first active BMD patrol (Brown, 2005).

Army Elements.

The Terminal High Altitude Area Defense (THAAD).

THAAD is a complete system consisting of an interceptor, X-band radar, and fire control system tasked with intercepting short and medium range ballistic missiles (General Accounting Office, 2006a). The program was started by the Army in January, 1992 when the prime contract was awarded to LM and transitioned to MDA later in October (General Accounting Office, 2006a). THAAD is being developed in incremental, capability-based 2-year blocks (General Accounting Office, 2006a). MDA plans to hand over the system to the Army for limited operational use in 2009 (General Accounting Office, 2006a).

THAAD has faced several technical issues. Among them a primary technical issue noted by the GAO has been integrating its components such as the missile and software developed by different contractors. While THAAD was conceived to integrate

and has been included in separate missile defense architectures with Patriot Advanced Capability-3 (PAC-3), the two systems have not been tested together and were designed separately. THAAD was intended to augment the PAC-3 system by making at least 2 attempts at target intercept before activating PAC-3, which would be a back-up if the target got by THAAD (General Accounting Office, 1993).

THAAD has been restructured due to test failures (General Accounting Office, 2006a). As a result an aggressive test schedule has been set (General Accounting Office, 2006a). This schedule is probably unrealistic given integration errors have occurred within the THAAD system itself (General Accounting Office, 2006b). It is unlikely the system will successfully work initially with other BMDS elements based on these results.

Patriot Advanced Capability – 3 (PAC-3).

The PAC-3 is a complete system composed of an interceptor, fire-control system, and radar sensor (Lockheed martin missiles and fire control patriot advanced capability-3 (PAC-3) missile. 2006). Its primary mission is to intercept short range ballistic missiles in their terminal phase of flight (Lockheed martin missiles and fire control patriot advanced capability-3 (PAC-3) missile. 2006). It is also part of another program with extended capabilities to intercept air breathing threats such as cruise missiles, UAVs, and air to surface missiles.

The PAC-3 program started in 1983 with LM winning the prime contract in 1987. Raytheon was brought on board later to perform system integration. Government oversight is performed by the Army, its primary user community. As its name implies, this is a follow-on system improving over the Patriot system used (with debatable success) in the first Gulf War that was used to defend against short-range ballistic

missiles and aircraft (Larsen & Kartchner, 2004). The first system used an exploding warhead as the kill mechanism, which was replaced with hit-to-kill technology in the PAC-2 follow-on system in 1995 (Larsen & Kartchner, 2004). The current system has also been upgraded over time through configuration updates. The second upgrade integrated its communications with joint forces while its third configuration interfaced the system with THAAD. Early trials have been completed to integrate the system with other land, air, and sea-based sensors.

PAC-3 is the only BMDS element to see combat. It successfully performed against Scud attacks in Iraq in 2003 (Larsen & Kartchner, 2004).

Joint Elements.

Command, Control, Battle Management, and Communications (C2BMC).

The C2BMC is the integrating fire control system that links all elements of the BMDS together (General Accounting Office, 2006b). C2BMC pairs weapon systems with sensors and directs those weapons on a distributed network. The system will carry out the following functions (General Accounting Office, 2006b):

- Situational Awareness
- Capture and display tracking data from multiple sensors
- Compute impact point
- Display GMD assets on users computer screens
- Provide planning tools for battle management

C2BMC began development in the 1990s. C2BMC is operated by STRATCOM, a joint command, with its development contracted to LM as the prime with NG subcontracted. C2BMC is being procured through a spiral development acquisition

strategy (General Accounting Office, 2006b). It was originally going to be the single integration point for C2 physically located at the Joint National Integration Center, Schriever AFB, Colorado (General Accounting Office, 2006b). Now, C2BMC suites are being placed at various unified command headquarters (General Accounting Office, 2006b). C2BMC appears to be a gateway implementation for the disparate systems and their software as the elements all have different software, formats, and languages. An effort has been underway to standardize message formats, but since BMDS elements have mission areas outside missile defense, those systems push back on any change. The C2BMC has seen several integration successes operating with various elements of the BMDS and passing test data through the system. Whether it has passed the right data at the right time cannot be verified until an end to end operationally realistic test is carried out.

Ground-based Midcourse Defense (GMD).

GMD is a system of components. It includes ground-based interceptors commanded by a fire-control system and land, sea, and space-based sensors that provide targeting and tracking information (General Accounting Office, 2006b). The primary mission of GMD is the protection of the US against intermediate and long range ballistic missiles in mid-course phase of flight (*BMDS booklet: A day in the life of the BMDS*2006).

The current GMD program was started in 1996, but its concepts trace back to the first NMD systems described in Chapter 1 (General Accounting Office, 2006a). In 1998 Boeing was awarded the contract for integrating the pieces of the GMD system (Ground-based mid-course defense (GMD) segment. 2005). These included the GBI system under

development, an evolving C2 system with heritage prior to 1993, legacy land-based sensors undergoing upgrades (Cobra Dane in Alaska, Pave Paws in California and BMEWS in Greenland and England), the evolving Aegis sensors, a new sea-based X-band radar, and a space-based sensor not yet operational (SBIRS) (Ground-based mid-course defense (GMD) segment. 2005). To add to the complexity, each component has government oversight by a different military service. Even though cross-service communication is likely occurring at STRATCOM, this is done at a strategic planning level, with little to no input from the element tactical level that has the knowledge of what is working and what is not working. While the acquisition strategy for these components is supposed to be a spiral development supporting 2-year block upgrades, the reality is upgrades are fielded and tested simultaneously which may lead to rework (*BMDS booklet: A day in the life of the BMDS*2006; General Accounting Office, 2006a). This has occurred in the GBI boosters which were fielded prior to operational testing. After test failures, production quality was determined to be poor and the fielded boosters now require major overhauls which must be accomplished in the field (General Accounting Office, 2006a). This procurement method results in fielded operational weapons that have a high probability of not working when critically needed.

The hardest component is the control system which currently orchestrates an engagement (General Accounting Office, 1993). If this is the system's largest hurdle, combining legacy systems with new systems must contribute to the difficulty. For instance, GMD currently uses the Cobra Dane radar, a fixed (as opposed to swiveling) land-based radar developed in the 1970s (Ground-based mid-course defense (GMD) segment. 2005). In addition to requiring upgrades, the radar is incapable of participating

in validation tests due to its orientation (General Accounting Office, 2006b). Additionally, the space-based sensor (SBIRS) planned to provide critical queing information to the fire-control system has yet to be put in place or tested itself (Ground-based mid-course defense (GMD) segment. 2005).

Kinetic Energy Interceptor (KEI).

KEI is a common interceptor being developed to destroy medium, intermediate, and intercontinental ballistic missiles in the boost and midcourse phase of flight (General Accounting Office, 2006a). Additionally various launchers and fire control systems are being designed for use with it (General Accounting Office, 2006a).

The program was started in October of 2002 and is being developed by NG and Raytheon to potentially replace all interceptors in BMDS elements (General Accounting Office, 2006a). While the program is supposed to follow the MDA acquisition strategy of spiral development supporting 2-year block upgrades, the program has already had its requirements review delayed 3 years due to funding cuts (*BMDS booklet: A day in the life of the BMDS*2006; General Accounting Office, 2006b). Additionally, the program has already been restructured twice in four years (General Accounting Office, 2006a).

The program hopes to create a standard system easily integrated into the various elements (*BMDS booklet: A day in the life of the BMDS*2006). To do this, the program is taking tested technologies from various BMDS elements (General Accounting Office, 2006a). It is unclear whether this will help compatibility later, or hamper it in the near term since the technologies are not necessarily compatible to begin with. Either way, the program's low level of maturity provides the opportunity to actually design a system with

future integration in mind. This is already occurring as a GAO reports that integration and hardware manufacturability are already being dealt with.

Summary.

The BMDS is composed of several elements. While all the elements are ultimately overseen by the MDA, most are primarily managed by a single service. Additionally, at least one of four common contractors is primarily involved in all of the elements. Several of the elements are based on legacy systems, and even the newest "original" elements are based on decades old concepts with all the prejudicial preconceived ideas guiding their development. These systems are supposed to come together to create an integrated system, but almost all were designed in isolation of each other. After years of development some are finally being integrated together through various piecemeal tests. The most important element for integration is the C2BMC which is providing a gateway for the various systems to communicate. However, there seems to be a problem. Much of the literature reports capability of single elements communicating with other single elements, and not necessarily through the BMDS. This implies there is no cohesive integration plan that all elements have been made aware of or signed up to. So, despite an entire element program being devoted to integrating the pieces, it is unclear how these legacy and new systems will come together.

Evolution of Computer-based Information Systems and Information Management

Many of today's IS are complex computer-based systems integrated into a vast network that spans the globe. To understand how these systems are managed and used, it

is useful to briefly examine their evolution. To do this, we look at how computers (used to manipulate information) evolved as well as methods for managing them.

The first computers were costly, standalone machines, with limited memory and processing capability, used for single functions such as calculation and code-breaking (Galliers & Leidner, 2003; Laudon & Laudon, 1997). These monoliths filled entire rooms and were very expensive (Galliers & Leidner, 2003). Additionally, computers could not switch from one function to another. So, while companies used information for multiple processes, the computer limitation forced redundancy in departments (Galliers & Leidner, 2003). Additionally, due to the capitol investment in these machines, companies were reluctant to change processes, since that could require a whole new machine (Galliers & Leidner, 2003). This established a mentality of using machines as much as possible to squeeze out the investment. It also meant new processes had to incorporate the old way of doing the machine's function.

Soon a second generation of computers emerged using transistors instead of vacuum tubes, but was still assembled by hand keeping the price high (Laudon & Laudon, 1997). These computers gained commercial use for automating single processes such as clerical work including payroll and billing (Galliers & Leidner, 2003; Laudon & Laudon, 1997).

From 1964 to 1979, the third generation of computers brought many changes (Laudon & Laudon, 1997). Miniaturization began with printing thousands of transistors onto a single silicon chip (Laudon & Laudon, 1997). Mainframes became common in most corporations and additionally began to be linked to remote users (Galliers & Leidner, 2003). This required software for the common user and in turn management

systems to monitor and control remote users' access (Laudon & Laudon, 1997). In addition to the remote terminal, computers made the leap from the floor to the desktop in the early 1970's (Galliers & Leidner, 2003). Next, individual departments or divisions began networking their computers to a central computer (Laudon & Laudon, 1997). With more people using computers, the market grew, prices dropped, and smaller companies soon were able to acquire the processing capabilities previously only held by large corporations (Galliers & Leidner, 2003).

1980 marked the start of today's computer generation characterized by integrated circuits and continually falling costs (Laudon & Laudon, 1997). This allowed for every employee to have a desktop computer of their own (Laudon & Laudon, 1997). Interestingly, despite department networks existing (recall the remote terminals linked to a central machine) desktops were not initially connected to one another (Laudon & Laudon, 1997). Additionally, since prices were so low, unit funds were used to purchase hardware and software (Wilson, 1993). This meant there was no strategic view of what was being purchased throughout an organization. As such, since this was on an individual basis, it led to multiple types of computers and software dispersed throughout the organization (Wilson, 1993). The only way to eventually link these disparate networks was to use gateways which were expensive, hard to maintain, slow and inefficient (Laudon & Laudon, 1997). Gateways were systems that could take the input from one system and translate it so the receiving machine could understand that input. In the 1990's organizational networks started appearing, however, and architectures for the entire enterprise are now used (Evernden & Evernden, 2003).

As computers evolved an entire cast of workers evolved to manage and design the systems, including programmers, systems analysts, and IS managers (Laudon & Laudon, 1997). Perhaps the most influential person, however, was the non-technical user who needed to share information with others. With non-technical users came the trend of non-technical people providing requirements to technical people (Galliers & Leidner, 2003). This started the issue of communicating between two groups that spoke different jargon. The result was misinterpretation of requirements leading to systems that did not fulfill the non-technical users desires (Galliers & Leidner, 2003). This set the stage for the antagonistic environment that would develop between "business people" and "IT people".

In efforts to mitigate the chaotic environment of computers that couldn't share information with each other, formal methods for designing systems were created that included requirements generation and software engineering (Galliers & Leidner, 2003). To oversee these processes the discipline of project management came about (Galliers & Leidner, 2003). In parallel, as technology grew and the capability of computers grew, so did the size and complexity of projects, but with no room for the users' inputs (Galliers & Leidner, 2003). The paradigm of division of labor persisted in organizing IS departments where programmers, system analysts, and users were physically separated, developing their piece of the system in isolation (Galliers & Leidner, 2003). This obviously led to difficult integration problems later which, in turn, caused budgets and schedules to be exceeded (Galliers & Leidner, 2003). One of the integration issues was that no standards were in place for programming leaving programmers to do as they saw fit (Galliers & Leidner, 2003). Then, in the early 1970's IBM invented the idea of structured project

teams with integrated management which brought the pieces together while they were designed (Galliers & Leidner, 2003).

As computers and the management systems to design computers as parts of integrated systems evolved, the substance they were used to manipulate evolved as well. In the late 1960's the focus changed from processing raw data to the data itself (Galliers & Leidner, 2003). As people began trying to share the data, they started recognizing the information redundancy issue. The idea appeared that a basic set of data used for many applications could be maintained in a single location, and thus a data management system was born (Galliers & Leidner, 2003). By the end of the 1970's data was viewed as a resource. This view fostered the database system and representation of data in a hierarchy (Galliers & Leidner, 2003). Soon the limits of hierarchies were identified and relational databases were created.

Over the past 60 years the equipment, resource, and people involved in information systems have evolved. They started out as isolated, singular entities, and grew into integrated communal systems adding up to be more than the sum of their parts. Computers started out as monolithic machines in a room with limited singular functions and capability and turned into a vast network of integrated components that is flexible and adaptable and capable of several functions. Information grew from instances of unsharable data to warehouses of information accessed by many users for multiple purposes. People who were once isolated in their small compartments have had their walls knocked down. They have been integrated as components of a team to tackle any problem presented from a system-wide view.

Parallels Between Information Systems and the Ballistic Missile Defense System

After reviewing the evolution of IS and the BMDS many similarities emerge. Both systems began as stand-alone entities with single functions. The components that evolved into integrated systems started as complex, intricate machines. As technology improved, capability also grew. With new capability came new diverse requirements to fulfill. Both systems saw a need for project management as complexity became more and more difficult to manage. Along with growing costs, expectations rose. This resulted in pressure on both systems to perform and to get the most out of those systems for as long as possible. This pressure solidified the need for a disciplined approach to project management. For the BMDS elements, project management took the form of systems engineering, a technical form of management.

As IS evolved an IM culture developed and IM subcultures (i.e. programmers, IT, system designers) developed. IS started out with computer engineers and technicians. Then, programmers, system analysts, information managers, and several other functional positions appeared. Each of these positions, while interconnected, had individual specialties with their own language and perspective. The BMDS elements, meanwhile, did not form cultures in the same way. Since military members move positions from time to time, the culture was not element specific, but service specific to that element. Still, many other cultures exist within the military and service culture. For example, SBIRS and STSS have a military culture, Air Force sub-culture, and space sub-sub-culture. Additionally, within the program there is a contracted company such as Boeing with its own culture, and government civilians with their own culture. All of these groups have

been isolated in the past but have been recently brought together with the advent of the integrated product team composed of military, civilian, and contractor members.

Another similarity which is a consequence of developing from stovepipes is inability to integrate. As IS grew in isolation (until it became possible to link the individual departments), they incorporated disparate equipment and software. When the time came to integrate, the individual IS were found to be incompatible. Not wanting to waste their investment, instead of creating a plan and procuring machines that could talk to each other, companies invested in gateway products to make the various machines communicate. The BMDS has seen the same development. With the investment of tens of billions of dollars, the DoD has decided to further invest billions to create workaround solutions and patches to make the various elements communicate. This has been embodied in the C2BMC. The IM world learned it is better to build a system from an enterprise perspective with a planned architecture incorporating standards and other IM Principles.

Information Management Principles

There are several recurring themes or principles in IM in general. But, there are no standard set of concrete principles. To determine if IM principles apply to the BMDS, a literature review was conducted to compile a list of IM principles that could be integrated into a model for application. Upon conducting a literature review of 14 sources composed of articles, texts, a university, and two military services, a list of common principles were compiled. From this list nine of the most prevalent principles

which may be useful to the BMDS, but not being explicitly applied were selected. The nine principles and their frequency of appearance in the literature are shown in Figure 1 below. Additional principles were mentioned but were either not appropriate for this thesis or too overarching. For instance, the principle of security was mentioned multiple times, however, the BMDS is definitely using this principle with great care as a military system. The nine principles are not necessarily being accounted for in the BMDS and are closely, if not exclusively, tied to IM. Finally, the principles are not isolated, but heavily interrelated and interdependent.

Information Strategy.

According to Evernden, the lack of a strategic view is the most costly problem that today's organizations face (Evernden & Evernden, 2003). Strategy is additionally important to ensure the systems meet their goals. IS implemented at the direction of an information strategy is a competitive weapon that can be used proactively (Gordon & Gordon, 1999). As computers, which are supposed to help us manage information, have become more capable, people have filled them with larger quantities of complex information that needs to be managed and exploited (Wilson, 1993). Instead of using the overwhelming information as a weapon to exploit, a gap has formed from this volume between the amount of information available and the capability for users to internalize it for use (Gordon & Gordon, 1999). The answer to this problem may be an effective information strategy.

INFORMATION MANAGEMENT PRINCIPLES									
REFERENCE	Information Strategy	Information Technology	Change	Value	Alignment	Standards	Culture	Information Architecture	Information Life Cycle
Galliers	X	X	X		X		X		
Auster	X	X		X	X	X	X		
Evernden	X	X	X	X		X	X	X	X
Wigand		X	X	X		X			
Wilson			X	X			X		X
Laudon	X		X	X	X		X	X	
Gordon	X	X	X	X	X	X		X	
Robertson	X		X		X		X		
DOE				X	X	X			
Navy	X	X			X	X			
Monash University	X	X		X		X			X
Oceanic Commission	X	X							
Symons	X				X				X
SAF/XC	X	X	X			X		X	
Frequency	11	9	8	8	8	8	6	4	4

Figure 1. IM Principles Compiled from Literature Review

Information Strategy is a specific derived strategy that affects goals, operations, products, services, and environmental relationships to aid the organization in gaining an edge over competition (Laudon & Laudon, 1997). It is derived from the corporate business strategy (Galliers & Leidner, 2003). The plan supports the overall organizational strategic plan describing pertinent systems development, rationale, current status, an IS/IT management strategy, implementation plan, and budget. This also addresses impacts on organizational structure, authority, and processes (Laudon & Laudon, 1997). A Strategic IS Plan is derived from the information strategy to determine Information Technology (IT) needs which will support the information and business strategy (Galliers & Leidner, 2003).

An effective information strategy must account for external environmental changes as well as existing organizational capabilities (Laudon & Laudon, 1997). It should also account for the organization's culture (Gordon & Gordon, 1999). It can be

created analytically such as from derived requirements of the business and information strategy, it can be created to specifically address a specific problem such as a poor understanding of competitors, or it can represent political influences (i.e. written with a bias towards implementing a preconceived technical solution) (Galliers & Leidner, 2003). One formal process conducted to create the information strategy is enterprise analysis, which asks managers what information they need, how they use information, where they get that information, the environment it is acquired in, the purposes their information fulfills, and their method for decision making with the information (Laudon & Laudon, 1997). Inputs should come from many departments (Galliers & Leidner, 2003).

To have a chance of actually being implemented, information strategy must be accomplished by senior leaders, not a low-level IT manager (Wilson, 1993). These high-level executives will set the long-term policies and objectives the information strategy is supporting (Gordon & Gordon, 1999). Further, what is key to information strategy is not just that it is derived from the organization's business strategy, but that it is considered during the formulation of the organization's overall strategy. This coordination will strategically align the business and information strategies (Galliers & Leidner, 2003). It makes sense to do this since a good information strategy will impact the business strategy (Galliers & Leidner, 2003). Information Strategy takes into account all the following areas and organizes them like pieces of a puzzle. Information Strategy is not a stagnant plan however; it must be reformulated regularly.

Information Technology.

As the history shows in CH 1, IT has been the focus of organizations' IM efforts. Corporations have made large investments in IT, but not IM (Evernden & Evernden,

2003). However, IT has typically failed to produce the results in productivity or in profits (Evernden & Evernden, 2003). In fact, the very systems that are supposed to help us manage information often cause new issues by increasing the amount and complexity of the information requiring management (Wilson, 1993). Even worse, the information may not meet the needs of the user (Gordon & Gordon, 1999). The lesson organizations seem to refuse to learn is that IT is not a solution, but an enabler (Evernden & Evernden, 2003).

Wal-Mart became a giant, not by using the latest IT innovation, but by wisely using organizational knowledge (Evernden & Evernden, 2003). Before purchasing IT the organization must understand the information important to the organization and its required structure (i.e. develop an IA) appropriate for the organization (Evernden & Evernden, 2003). In looking at the major IT investments of the last five years (data warehousing, data mining, business intelligence, customer relationship management, e-commerce, enterprise applications, KM or corporate intranet/extranets), they all use information (Evernden & Evernden, 2003). Understanding the information allows IT to be employed optimally. Simply automating current processes does not yield IT's full potential (Laudon & Laudon, 1997).

In addition to the information and IT used to manipulate that information, the people aspect must be accounted for as mentioned above. In 1992 Microsoft and the Institute of Management conducted a survey that found despite a majority of managers acknowledging the importance of IT, almost all feared it (Wilson, 1993). This shows that IT cannot fulfill its potential unless organizations support training their people (Evernden & Evernden, 2003). Additionally, with technology continuously changing, technical

skills must also be continuously updated (Gordon & Gordon, 1999). Laudon further adds that for IT to be accepted the organizational environment, structure, culture and politics must be accounted for (Laudon & Laudon, 1997).

When IT is used properly, it can have significant impact. IT can transition an organization into a flat structure using decentralized control composed of flexible generalists who use instantly available information to produce mass-customized products and services (Laudon & Laudon, 1997). In addition to flat structures, IT allows team-based management through lateral communication (Gordon & Gordon, 1999). IT allows automation, rationalization, reengineering, and paradigm shifts (Laudon & Laudon, 1997). But all affects must be accounted for. Instituting enterprise networking, for instance, must address: loss of management control (centralized control vs. end-user decision making and productivity); organizational changes (reengineering vs. cultural backlash); hidden costs (additional highly paid tech support vs. less workers); and difficulty of network reliability and security (Laudon & Laudon, 1997). IT is not a cookie cutter solution, but an enabler to a well thought out and planned solution to strategic change.

Change.

While Change may seem to be an overarching principle like leadership, it is critical to IM. The principle of Change describes the nature of information, thus information's life cycle described below and the requirement to update the Information Strategy mentioned above. I will discuss three key components: change management, change in the information market, and organizational change.

Change Management.

Change Management provides a plan for implementing new ideas and innovation. When changes such as new technology are required, impacts to the organization (i.e. structural change, alignment) occur which must be managed. According to Galliers, this role may be the most important in an IS department as change management can determine how successful IT is implemented (Galliers & Leidner, 2003). Areas impacted include: business processes, the information architecture (IA), organizational structure (i.e. staffing levels), power structures (i.e. who controls what information), and culture (Laudon & Laudon, 1997).

The person who carries out this function must have credibility and a fundamental understanding of the information strategy and how end-users operationally accomplish its objectives and goals (Galliers & Leidner, 2003). This person is called a change agent and is often a part of the IS department (Galliers & Leidner, 2003). The change agent interacts with those affected, especially groups where power is shifted (Laudon & Laudon, 1997). Since changes from an information strategy can affect the whole organization, this person must understand more than just the IS/IT department (Galliers & Leidner, 2003). Change agents must be technically competent, but able to relate to end-users to effectively accentuate the positives of the new changes (Galliers & Leidner, 2003). They must be able to do this by selecting the right tool; political advocacy, facilitation, or technical expertise (Galliers & Leidner, 2003).

This is necessary because while some employees may welcome change seeing its benefits, others will resist perceiving certain aspects of the change as detrimental to their interests (Laudon & Laudon, 1997). Resistance can come in many forms. Active

resistance may take the form of causing errors, disruption, turnover, and possibly sabotage (Laudon & Laudon, 1997). Even those who seem open to the changes may avoid new systems (Laudon & Laudon, 1997). The change management section of an information strategy should include ways to overcome these forms of resistance through end-user participation, training, management coercion, and incentives (Laudon & Laudon, 1997). Laudon and Evernden agree that training is an important aspect of managing change (Evernden & Evernden, 2003; Laudon & Laudon, 1997). The plan should also address the organizational culture (Galliers & Leidner, 2003).

Changing Information Market.

As stated above, the environment in which an organization operates is constantly changing. Globalization alone has significant impacts to organizations such as increased competition which forces companies to reevaluate the quality of their goods and services (Gordon & Gordon, 1999). This competition is brought by borders disappearing as information flows without regard to political or geographic limits (Wilson, 1993). The quantity of private information traveling freely doubles every six years (Wilson, 1993). Technology in general is changing at such a pace managers must continuously assess how well their existing technology satisfies their information needs (Gordon & Gordon, 1999). The internet has been a primary player bringing buyers and vendors together in the new global economy (Laudon & Laudon, 1997). These environmental changes lead to organizations having to look at their organization and identify strategic changes for implementation.

Organizational Change.

Organizational Change is a specific consequence of changing information and the changing IT which helps us manage it. As stated above, the environment has changed to a global market which complicates business operations, yet demands more flexible and responsive companies. This increase in complexity requires new IS (Laudon & Laudon, 1997). The power of these systems has grown more rapidly making it difficult for organizations to apply it optimally since organizational change occurs at a slower pace due to cultural inertia (Galliers & Leidner, 2003). The changes required include altering their structure and reallocating control of information (Laudon & Laudon, 1997). Organizational structure is made of the division of labor, coordination of positions, and the formal reporting relationships (Gordon & Gordon, 1999). Traditional organizations use hierarchies which restrain the flow of information since it stops at each level of structure (Gordon & Gordon, 1999). Using IT, executives can instantly make information available throughout the organization increasing their span of control, and eliminating the need for much of middle management in traditional structures (Gordon & Gordon, 1999). This flattens the organization and makes it more responsive since feedback can also be obtained more quickly.

Innovative IS drives changes in strategy and processes as well (Laudon & Laudon, 1997). All these changes must be aligned for synergy as described below. This all links back to information. When an organization changes proactively, in a planned manner (as apposed to a reactionary, haphazard manner), they use information about the required change. It is this information that must be used to construct the new IA and organizational structures (Evernden & Evernden, 2003).

Value.

Value is the characteristic of information that makes it important to organizations as a resource and motivates the other principles to be applied. The monetary value of information is the primary driver leading to its utilization. It is easy to see how information can have monetary value. Profits can be obtained through the laws of intellectual property such as patents and copyrights (Wilson, 1993). Additionally, information can be traded much like a commodity such as corn, autos, or machines (Gordon & Gordon, 1999). While this may seem obvious and straight forward, patents that are valuable to one person at one time may not be so to another person at another time. The value depends on interpretation and experience (Evernden & Evernden, 2003). For example, the patent for the internal combustion engine was once very valuable to Ford, but has no value to a banking company today.

To have monetary value, information must have certain characteristics that make it good, useful information. Organizations only value information that is relevant, timely, consistent, and accurate (Galliers & Leidner, 2003). It must also be accessible, reliable, and secure (Gordon & Gordon, 1999). Further more, it must be complete, clear, and useful in decision making (Wilson, 1993). The profitability of companies depends on good decision-making throughout an organization, which depends on the information available throughout the organization (Wilson, 1993). Finally, organizational information must be of good quality. This means it is accurate, precise, credible, current, pertinent, relevant, reliable, simple, and valid (Evernden & Evernden, 2003). And for customers it is available at the right time, right place, and correct format, lest they will go somewhere else (Gordon & Gordon, 1999).

The way organizations get information to the organization is through the IS. The IS is also how organizations dispense valuable information. Business success can depend on an IS that perpetuates quality information and makes its management easy (Laudon & Laudon, 1997). As mentioned above, information must be relevant. To ensure information is relevant, an IS must only contain pertinent information. That is, it is equally important to omit or delete unimportant information, which if available can distract users (Galliers & Leidner, 2003).

Alignment.

Studies have repeatedly reported that the alignment of IT and organizational objectives is a major concern of IS managers (Galliers & Leidner, 2003). Additionally, senior managers (other than those in IS) agree that alignment of IS with the business strategy is critical (Gordon & Gordon, 1999). Studies have also shown that it improves organizational performance (Galliers & Leidner, 2003).

Gordon defines strategic alignment as the "fit" of organizational goals and objectives with its IS. A similar explanation describes how well the IT department's mission objectives and plans and business mission objectives and plan support each other (Galliers & Leidner, 2003). Further, alignment can have an intellectual and social dimension (Galliers & Leidner, 2003). It's the social dimension that is influenced by culture and thus much harder to address (Galliers & Leidner, 2003). To gain social alignment, the business and IT cultures within an organization must have shared domain knowledge, an understanding of what the other culture does and the significance of their contribution to the organization (Galliers & Leidner, 2003). Social alignment contributes to intellectual alignment, the degree to which IT and business plans are interrelated

(Galliers & Leidner, 2003). Four factors influence this state: shared domain knowledge, IT implementation success, communication between IT and business departments, amount of coordination between the business and IT planning process when alignment is determined (Galliers & Leidner, 2003).

There are six types of alignment: Strategic (between business and IS strategies), Structural (between business and IS structures), Business (between business strategy and structure), IS (between IS strategy and structure), and cross dimension (business structure and IS strategy; business strategy and IS structure) (Galliers & Leidner, 2003). These can be reached by looking at the organizational strategies, structures, and planning methods or the players and their values, interpersonal communication, and level of shared domain knowledge (Galliers & Leidner, 2003). They are not static, but dynamic due to a changing environment which may require new strategies affecting the organizational structure (Galliers & Leidner, 2003). Because these aspects rarely change at the same pace, only short term alignment is realistically achievable (Galliers & Leidner, 2003). This means, like strategy (and in parallel with it), alignment must be reevaluated periodically. Important to note is that alignment changes that are revolutionary (large departure from the current state) are hindered by cultural and structural impediments requiring well planned change management. These revolutionary changes are forced by environmental shifts, sustained low performance, influential outsiders, new leadership, and perception transformation (Galliers & Leidner, 2003).

Standards.

Most people understand what a standard is. However, their importance is taken for granted. Standards can increase efficiency and flexibility by allowing systems to

share information and processes, creating a single system everyone and anyone can use (Gordon & Gordon, 1999). This means, people can be used in more roles since they all can operate the system. Without standards information and processes often cannot be shared. Confusion and misunderstanding takes place because words have similar, but different meanings (Evernden & Evernden, 2003). For example, what is the difference between an estimate and a quote? This distinction may vary depending on whether you ask an insurance salesperson or a mechanic. This means that context, which places the information in the proper situation providing the correct meaning, is extremely important (Evernden & Evernden, 2003). The responsibility of establishing standards in an organization resides with the information professionals who are obligated to create and establish them through strategic planning as business information needs evolve (Gordon & Gordon, 1999). When creating standards for a single purpose, such as missile defense, the most appropriate format must be used to ensure information is interpreted as intended, data is not confused, and misinformation is not created (Evernden & Evernden, 2003). As such this principle must be instituted for any action to be carried out. This function is carried out for many technical disciplines by the International Organization of Standards (ISO).

In the context of IS, language is the primary element of design and operation (Evernden & Evernden, 2003). For global systems, standards must be applied to hardware, software, and communication formats (Laudon & Laudon, 1997). One way this is being done is by creating open systems. Open systems enable different equipment and services to work together because they are built on public, nonproprietary standards and protocols everyone can access and understand (Laudon & Laudon, 1997).

Finally, not only should standards be applied to communicating, but also in measuring and validating information and the systems it resides on. To improve, change must occur. To determine if the right change occurred, some measurement must be made to validate the change (Wilson, 1993).

Standardization is a trade-off. While it can lead to flexibility, it does so by placing limits (i.e. you can only use one system for everyone to understand it) (Gordon & Gordon, 1999). Additionally, there are cultural impacts (Gordon & Gordon, 1999). A company choosing an Apple OS may have to wage a big fight against the Windows culture for it to be implemented. In general, standards are necessary and beneficial. The trick is to strategically determine how much and which ones to use for each organization.

Information Architecture.

All organizations have an IA whether formally planned or by default (i.e. the natural, yet chaotic, result of buying several computers and automating a file system) (Evernden & Evernden, 2003). It is the form IT takes to achieve the goals of the information strategy (Laudon & Laudon, 1997). If well planned, it can be the most powerful tool for an organization (Evernden & Evernden, 2003). A default IA may be a decentralized architecture characterized by isolated islands of information where data is not shared, utility is limited, repeated entry is required, and inconsistencies may occur (Gordon & Gordon, 1999). The hidden costs of informally creating an IA are much more than that of a strategically constructed IA making the planning time worth while (Evernden & Evernden, 2003). Using information without understanding the IA is analogous to using money without understanding the accounting structure (Evernden & Evernden, 2003).

IA is necessary for large, complex organizations where change is constant. Additionally, when there is potential for economies of scale and a high degree of coordination is required, IA is beneficial (Evernden & Evernden, 2003). Organizations that need IA deal with great amounts of complex information, exist in an unpredictable environment, provide information based products or services, share information through a supply chain, and have consistently changing information needs (Evernden & Evernden, 2003).

One thing to remember is that there is no single IA that works for every organization, and realistically, each organization will have a slightly unique IA (Laudon & Laudon, 1997). What's more, due to change, organizations will need to update their IA periodically in parallel with the Information Strategy (Evernden & Evernden, 2003). Organizations can change their IA four ways: Optimization, which improves the IA; Augmentation, which extends the IA adding value or using it in a different way; Transformation, which replaces the IA with a new architecture; and Creation, which presents totally new structures (i.e. new staff positions) that didn't exist before (Evernden & Evernden, 2003).

So what is an Information Architecture? According to Evernden:

> IA is a foundation discipline describing the theory, principles, guidelines, standards, conventions, and factors for managing information as a resource. It produces drawings, charts, plans, documents, designs, blueprints and templates, helping everyone make efficient, effective, productive, and innovative use of all types of information (Evernden & Evernden, 2003).

IA has the following characteristics: it views information as a resource; it affects everyone, not just the IA designer; it accounts for all kinds of information (not just IT); it

serves as a foundation for organizational structure, information flow, and processes; it's a discipline that requires expertise (Evernden & Evernden, 2003). The most important aspect of IA is that it requires an organization to know WHAT information is important (i.e. has value), and that determines the scope and the required IT (Gordon & Gordon, 1999). The tendency is for organizations to not understand ALL the information they need to manage, thereby creating insufficient architectures (Evernden & Evernden, 2003). Additionally, IAs fail because of a lack of commitment, poorly defined requirements (i.e. not knowing what information is used), overly complex planning tools for using information, ambiguous projects (i.e. purchasing IT without a plan), not knowing how useful available information is, and not implementing a process for keeping information up to date (i.e. not understanding the information life cycle) (Evernden & Evernden, 2003). IA enables everyone to have the right information available and know how to use it (Evernden & Evernden, 2003).

Culture.

Culture is perhaps the most pervasive and underestimated area in information management. Culture is defined by a set of assumptions shared by a group which governs its actions. Within the organization, culture consists of the core beliefs of how things should operate (Laudon & Laudon, 1997). This organizational culture serves as a unifying force that generates a common, mutual understanding on procedures, processes, and policy (written and unwritten), and is also a strong barrier to change (Laudon & Laudon, 1997). The organization's culture is greatly influenced by the market environment and senior managers (Galliers & Leidner, 2003).

The nature of culture, intangible beliefs and behaviors, has concrete consequences in organizations. Culture manifests itself in symbols, organizational structures, power structures, control systems, and informal (but set) ways of doing things (Galliers & Leidner, 2003). Corporate processes no longer necessary persist for no explainable reason (Evernden & Evernden, 2003). For example, entering data by hand instead of scanning it in. This example also serves to demonstrate culture's resistance to technology. IS are sociotechnical systems that include people as well as technology (Laudon & Laudon, 1997). This implies that new technology has social impacts, which means the people who use it must be taken into account and thus their culture must be taken into account (i.e. change management) (Galliers & Leidner, 2003; Laudon & Laudon, 1997). A cultural gap has been identified between IT and business people which has been a major cause of system development failures (Galliers & Leidner, 2003). If this is not done, the culture in the form of unconscious bias will be embedded in the IS through IS implementations that support the culture (Laudon & Laudon, 1997). To combat this, an organization must understand artifacts, which are the remaining beliefs based on forgotten complex factors (Evernden & Evernden, 2003). This is classically exemplified by a new employee asking why a process is done a certain way, and the supervisor replying it's just the way it's always been done.

Culture has been discussed on a group level, but it must also be understood that cultures exist on the subunit and even individual level (Galliers & Leidner, 2003). Two important subcultures are individualistic and collectivistic. An individualistic culture has a loose network with soft ties where people worry about themselves first and the group second (Galliers & Leidner, 2003). A collectivistic culture puts the group first to achieve

a desired sense of belonging (Galliers & Leidner, 2003). Individualistic cultures are results oriented and private as opposed to collectives which are process oriented and open (Galliers & Leidner, 2003). This affects information flow and power structures. The individualistic culture will hoard information to keep power, while a collective will allow the free flow of information to promote organizational gains (Galliers & Leidner, 2003). Recognizing culture types will aid in identifying barriers to changes such as organizational restructuring (Galliers & Leidner, 2003). Individualistic cultures will provide steeper resistance to flattening of organizations which requires/promotes information sharing. While culture can have many negatives such as being inflexible and one-track minded, they also provide stability and clear direction (Galliers & Leidner, 2003).

Information Life Cycle.

The discussion of value depicted information as a temporal entity with its importance dependent on timing. The Information Life Cycle is a framework for formally and proactively recognizing this aspect of information. Information in organizations is generated internally with a single purpose (Evernden & Evernden, 2003). Once this purpose is fulfilled, it is expired and no longer useful. Problems arise when information is retained beyond its useful life resulting in inaccurate records which are not only useless, but could be detrimental. Information's life cycle is accounted for in an IA which identifies a timeframe for when specific information is useful (Evernden & Evernden, 2003).

Summary.

These nine IM principles were structured to create the framework depicted below in Figure 2 for how to institute and carry out IM. The model shows that Information Strategy is the overarching strategic plan for instituting the other principles. The Change Management Plan explains how to deal with change (i.e. structure, processes, marketplace) and cultural issues. The IA defines what information is valuable; correct organizational, process, and strategic alignment; IT which enables the information strategy goals and objectives; applicable standards for the system; and the life cycle for information.

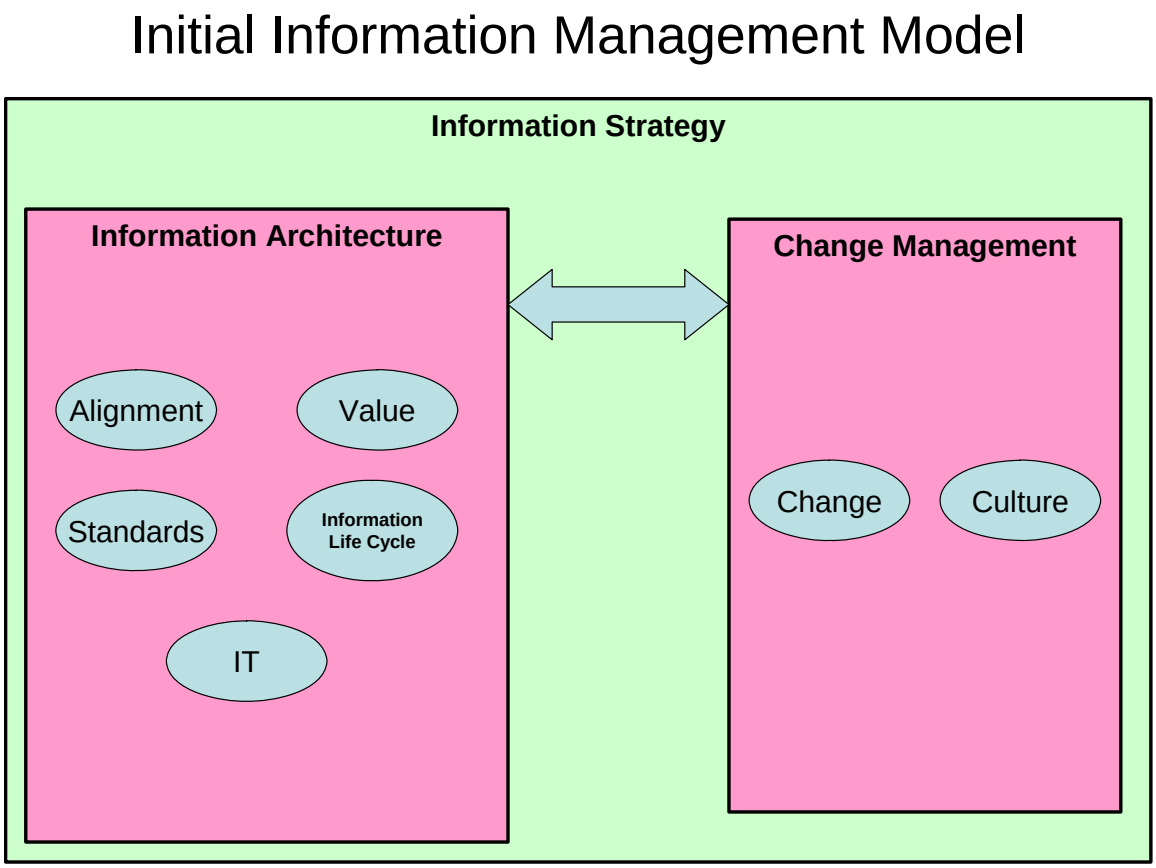


Figure 2. Initial IM Model Constructed from 9 IM Principles

III. Methodology

Thus far, this paper has depicted a model of the BMDS (group of disparate elements, legacy and new, integrated by the C2BMC element) and of Information Management Principles. To determine if the latter applies to the former outside expert opinions will be obtained.

This thesis seeks to determine if IM principles apply to the BMDS. Because this idea has never been entertained, it is desired to seek a valid and strong indication of its applicability. Therefore, a small group of experts with the experience and applicable knowledge will be sought to provide credible salient opinion on the thesis.

Through the Delphi Technique a group of relevant experts are used in a structured communication. Generally, the group is posed questions about a problem and then provides feedback. The feedback is collected and points of disagreement are noted. The group is presented the points of disagreement in an attempt to rectify these points. This process continues until general consensus is reached about the original problem (Linstone & Turoff, 1975).

The Delphi technique has some limitations. The group is composed of a small number of people. However, these people are experts. But, the experts must be carefully chosen to ensure their background is relevant to the subject area. Language must be carefully selected when communicating with the group to ensure objectivity and clarity, especially when presenting data of one member to the other members. The moderator must not ignore disagreements such that dissenters become frustrated and stop

participating in the group. The Delphi Technique can be time consuming if it is not the primary job of its participants (Linstone & Turoff, 1975).

The Delphi Technique is used to create a common credible opinion about a subject (Linstone & Turoff, 1975). Despite its possible challenges, the technique can provide a reasonable estimate of future fact. The technique has been used by the military, health industry, and many more around the world to make plausible projections about future implementations of strategic ideas (Linstone & Turoff, 1975). This thesis aims at projecting whether a new idea of how to manage a complex system would work. To do this, the Delphi Technique is a reasonable method.

A Delphi Group will be used to provide expert opinion on whether the model of IM composed of the nine principles applies to the BMDS and its integration. The group is composed of three experts. Expertise is defined by experience in their profession and with at least one element of the BMDS. The group has a mix of military, civilian contractor, and government contractor experience. Additionally a wide variety of technical and management experience exists.

The group will be presented with an executive summary of Chapters 1 and 2 which includes the Information Management model and BMDS description. Given this information, the group will be asked four open-ended questions about whether the principles are applied, the model's applicability, and the model's possible application to integrating the BMDS elements. With each question an example for clarification, and to spark dialogue, will be given. Upon receipt and synthesis of the initial responses, follow up questions will be posed presenting ideas from one member to the other members for comment and clarification. Based on a second round of responses a final round of

questions for clarification may be performed. The results of the Delphi Group structured communication will be presented in Chapter 4.

IV. Results and Analysis

A Delphi Group provided expert opinion on the applicability of IM principles to the BMDS. The members had experience in multiple elements of the BMDS. They had military and civilian experience. Members worked with and for companies contracted to design and build multiple elements of the BMDS. Work experience exceeded 20 years for all members. Engineering expertise was in the areas of missile defense technology. Additionally management background included training in Total Quality Management, Six-Sigma, and Lean. The members were presented a summary of the literature, and the information management principles shown below in Figure 3. With that information, they were asked to provide their expert opinion on the principles' applicability to the BMDS and its integration. Below are the results of that discussion with a brief summary in Figure 3.

DELPHI GROUP RESULTS			
	Round 1		Round 2
Model	Relavent	Being Applied	Being Applied
Information Strategy	X	Maybe	No
Change	X	No	No
- Culture	X	Somewhat	Yes
Information Architecture	X	Maybe	No
- Value	X	No Comment	No Comment
- Alignment	X	Somewhat	No Comment
- Standards	X	Somewhat	No Comment
- Information Life Cycle	X	Maybe	No Comment
- Information Technology	X	Poorly	No
Modifications	Add Security, Apply Model at 3 levels: System, Element, Inter-element		

Figure 3. Summary of Results from Delphi Group

Initial Delphi Responses

Application.

The Delphi group agreed that IM principles are already being applied. There were different opinions on which principles were applied and how effectively. All of the principles were identified as being applied except Information Strategy, which was specifically commented on as being weak or nonexistent. Additionally, at least one member felt IA was especially poorly applied throughout the system. Culture was said to be set at the Agency level which affected how information was valued and treated at the element level. Additionally, element culture was said to be developed early in program creation after a contractor is chosen.

Application of Non-applied Principles.

The group had different opinions on what principles were being applied. Information Strategy was restated as being absent, while the intent of the Information Strategy was stated to be carried out by other documents such as an Acquisition Strategy which addresses IT, structure, culture, and processes. Additionally, Culture was identified as being poorly understood by the acquisition community which may affect program execution.

An additional distinction was made between the element level and MDA level. Different principles are applied at varying degrees. For example, Information Strategy and IA are perceived to be more important at the MDA level and less so at the element level. They feel these should be flowed down from agency to element.

Another specific deficiency mentioned, but not agreed on, was Information Life Cycle. One member felt this was inherently taken care of by the system while another identified the importance of archiving lessons learned for producing future increments of the system. While this is being done in at least one element, it is not happening at the agency level which is in a better position to make effective use of this concept. The emphasis is on creation and use of information while disposal is overlooked or ignored.

Non-applicability.

The group unanimously agreed that all the principles were relevant and should be applied to the BMDS and the individual elements. Again, a distinction was made as to which principles were more important to the element and agency levels.

Application to BMDS Integration.

The group had varying ideas in this area. Two principles of the model came through as being clearly beneficial, however. Information Strategy is clearly perceived as being desired and necessary. One member explained that an information strategy could direct information flows creating an overall more unified flow. The idea of time phasing the information strategy with planned system changes was also offered. Further, the effect of not having an information strategy is to constrain elements to individual optimization. It also places each element in a reactionary mode with respect to the other elements. For example, without an information strategy that details how each element uses information from the other elements, individual elements are forced to assess possibilities as they become available. This means missed opportunities because they are not provided the ability to use all the available capability. They can only use what their

system (designed as is) will allow. Additionally, integration is hampered by elements that do not understand BMDS level objectives, needs, and requirements.

Information Architecture is also perceived as being beneficial (especially at the beginning of a program), but there was a sense of it not being quite as critical. This is because there is an implicit assumption that *an* architecture exists at a top level that is being worked toward. Additionally, the contractor is heavily leaned on to institute IA as well as the other principles of the model. Even so, they felt IA would aid in understanding issues vertically and horizontally. It would also aid in communications and defining the information flows.

Standards were pointed out as being a principle that could offer help. Here, the standards must be unambiguous such that all cultures (military, contractor, etc.) can understand them, and more importantly, that they remain consistent through time.

Additional Results.

Open-ended questions provided additional comments outside the area of the specific questions. The group identified possible changes to the model, barriers to its application, and some ramifications of the model.

Security was mentioned as an additional principle that should be added to the model. Security was pointed out as influencing, if not dictating, how the other principles were applied. For instance, technology may bring on changes that breach current security protocols. This was demonstrated in the military when cell phones began integrating cameras. Additionally, security scrutinizes all information generated. This scrutiny necessitates good IM practices.

As mentioned above, the BMDS has various hierarchical levels. The Delphi group identified that the IM Model can be applied differently at these different levels. The three levels are System level, Intra-element level, and Inter-element level. These three perspectives place different priorities on different aspects of the model.

Several barriers to implementing the IM Model were mentioned. First, while needed change was said to be quickly recognized, its implementation was slow due to current processes which require communication to many entities and a lack of adequate communications IT for flowing this information. Second, while standards are most effective when stable, technology used in the BMDS continues to evolve. Third, the culture of stovepiping still exists. MDA is perceived to be developing stovepipes in the elements fostering protectionist tendencies that contradict the need to integrate the elements. Despite a MDA directive to use multi-use technologies, finding the uses outside one's own element for technologies is low on the priority list with little effort expended toward it. Forth, the security environment is an especially difficult barrier to penetrate due to varying security classifications. Fifth, the entire Delphi group did not feel instituting the IM Model on their own was their responsibility. They felt it was their duty to carry out any directives, but those directives should be constructed by IM professionals at the BMDS level. Sixth, communication between contractor and government is impeded by hidden agendas.

Despite these barriers, there are motivating benefits to instituting the model. In addition to aiding integration efforts, Information Strategy could help cut costs and make organizations leaner and more efficient. Information Strategy would also specify necessary inter-element interactions.

Finally, starting early was stated to be essential. Instituting the IM Model early can be used to create and mold an IM culture. This can lead to improved communications and inter-element coordination. This could lead to identifying problem areas ahead of time. It can also serve to share information and get buy-in early for forecasted changes.

Second Round Delphi Responses

The initial responses received did not say that an Information Strategy document did not exist. Follow-up responses clarified that no one in the Delphi group has seen this document. However, they reiterated that functions of an explicit information strategy were carried out in the Acquisition Strategy and other plans derived from that strategy. Further, these functions were flowed all the way down to the end-user level. Additionally, these documents are updated twice a year, which further meets the intent of the information strategy. While these documents fulfill the functions of Information Strategy by instituting the IM principles, they do not do this explicitly. That is, the principles are not specifically called out. They are also applied by default through normal acquisition practices.

The Delphi grouped readdressed Culture which the group felt impacted the system. They confirmed that Culture is important and it influences the system in different ways such as contractor selection, manning, and system design.

Culture is factored in during contractor selection through evaluating the processes (including IM) the various contractors use. Those contractors with processes that align

well with the program office receive favorable scores in those areas. Past experience (i.e. with space or with the actual system) which is a part of the current contractor culture is also taken into account.

The operational system is also impacted by ensuring that different cultures can interact with the system. For instance, the system is designed for use by non-technical users, who would not understand all the cultural specifics (e.g. language, symbols, processes) of the technical engineering world.

Finally, programs are manned, to some extent, based on cultural bias. AF programs don't even consider bringing in other services to man their element program offices. They specifically stick with their own service. Additionally, contractors favor hiring engineers that have worked on other similar programs. This inspires these cultures to exhibit a closed community mentality resulting in a lack of information sharing. So, when one program makes a technological breakthrough that could apply to another element, that success and vital information is not communicated.

In the area of integration, Information Strategy was again emphasized as a major asset. The point was made that this needs to be created at the beginning of the program before a contractor is selected. This aligns the contractor making the element system with the service expected to operate it. Additionally, one member thought Information Strategy should be part of the Acquisition Strategy, as apposed to its own document. Further, not having an IA is hindering development progress.

While it is agreed that this model should have been consciously applied at the beginning of all the programs, some thought it cannot be formally instituted in programs already underway. Only future programs can have the model explicitly applied. One

reason for this is that the organizations are too resistant to change. Another reason is that elements that are in development with operational versions to be built later won't be integrated into the operational system.

Upon redirect, additional information was obtained. MDA has the means to communicate information directly to all elements via secure websites. It does not use this tool, however, to advance integration through information sharing pertinent to multiple elements. For instance, common standards are not listed for reference by all elements. Another interesting perception is that element culture is not established until operations begin. It is at that time that cultural alignment is determined.

Summary

The Delphi group believed that the IM principles are relevant, and some are being applied to their element and the BMDS. Various aspects of the model are being applied in varying degrees at different organizational levels. The IM Model would be beneficial to future systems, but cannot be realistically instituted in programs already underway because they are too resistant and slow to react to change. Additionally, attempting to enact the model (i.e. create an information strategy, IA, etc.) while simultaneously accomplishing the current scheduled work would cause any schedule to slip. Several barriers (e.g. change process, standards stability vs. new technology, stovepipe culture, security) to enacting the model were mentioned. The Delphi Group has not viewed a specific Information Strategy Document or Information Architecture, but while they agree these would be beneficial to integration, they also agree that their intent is being

carried out implicitly in other ways such as in the Acquisition Strategy Plan. Finally, Culture is not only important; it impacts the system in various ways. It, like the other principles, however, is not explicitly addressed. A new model based on the Delphi Group responses is shown below in Figure 4.

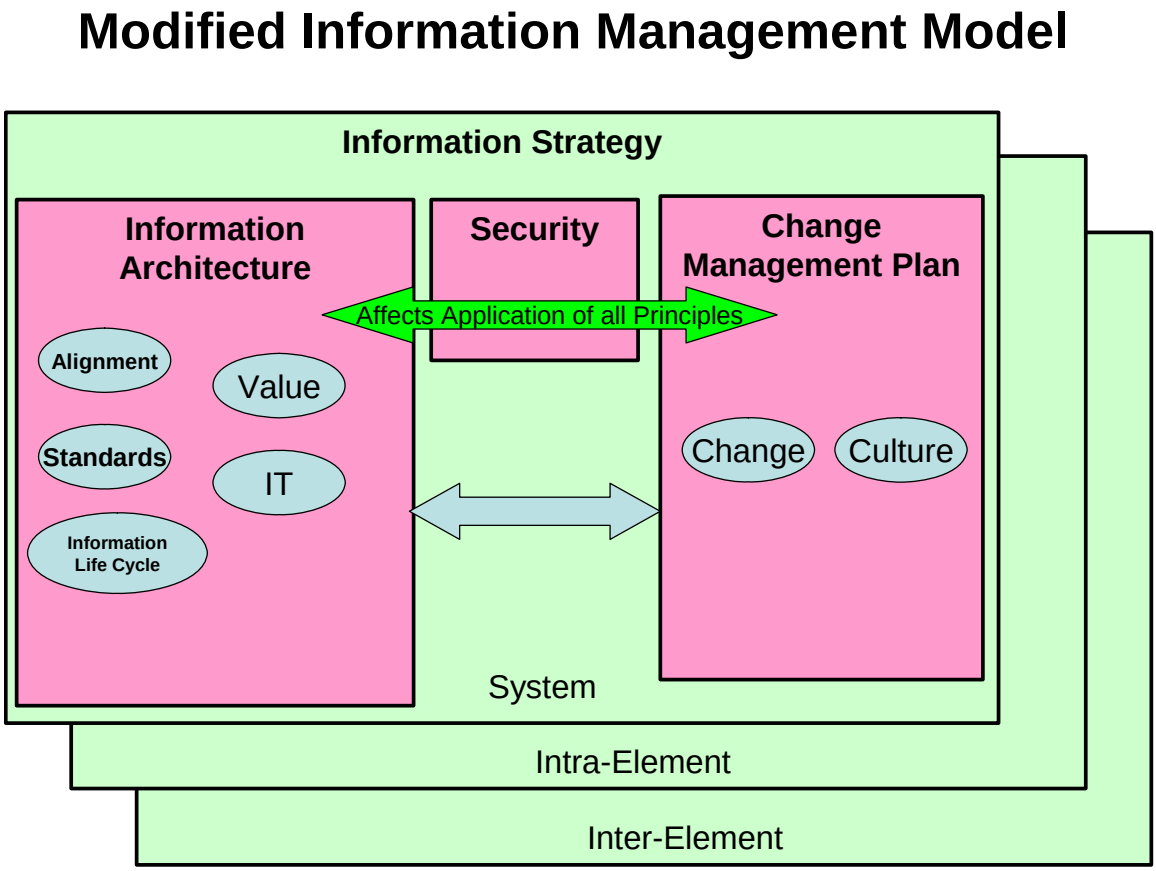


Figure 4. Modified IM Model Based on Delphi Group Responses

V. Discussion, Conclusion, Recommendations

The question of this thesis was if IM principles applied to the BMDS? Further, could they be applied to aid in the task of integrating the various elements? Similar to the evolution of IS, the BMDS has evolved from individual elements with singular functions to integrated networked systems with multiple functions. A former director of the MDA has stated that integrating these elements is a management problem, not a technical one. Much of the BMDS is a type of IS. Based on their responses, the Delphi group supported application of the IM Model constructed of IM principles to the BMDS.

Discussion of Delphi Results

The Delphi Group was presented the IM Model and asked four questions. They confirmed that the IM Model is applicable. Additionally, they revealed that aspects of the model are being applied. For instance, Culture is factored into source selections for BMDS element contracts. Additionally, some standards are specified in accordance with military standards and communications standards (e.g. operational frequencies). Also, processes are in place to identify needed changes.

The Delphi Group showed that while some principles of the model are being applied, none are being applied explicitly. That is, their functions are carried out through other means such as an Acquisition Strategy, but an actual Information Strategy and Information Architecture do not exist. This is important because implicit application of aspects of the model may not produce the full potential benefits of applying the model

explicitly. Without explicit application, the impact of one principle will not be identified with respect to the other principles. So, while the Acquisition Strategy may be updated periodically, alignment may not be adjusted or what makes information valuable redefined. Additionally, the model is created based on the principles being interrelated and interdependent. For example, if random standards are applied, they are not necessarily applied to the pertinent information or in the right way. Also, without an IA, there is no way to know if standards are applied across the system. Without an IA elements may apply different standards that aren't compatible.

One major aspect of the model the Delphi Group identified as not being applied is Information Strategy. This principle structures all the other pieces of the model. Therefore it was not surprising to find that the Delphi Group mentioned other principles in the model were poorly applied, such as IA and IT. The fact that elements are being constrained to optimizing themselves without input from other elements demonstrated the importance and relevance of Information Strategy and the model itself.

It was surprising to learn that while the Delphi Group felt the model would be beneficial to managing and integrating the BMDS, they thought this should only be done for new programs. If only new programs had the model applied, limited results would be expected since it is intended to span the entire system and define relationships between elements. What's more, a suggestion was to apply the model from three perspectives: system, intra-element, and inter-element. It would be difficult to apply the model to the system and inter-element if only new systems used the model. The three-level application idea had not been specifically included in the initial model.

Security was another addition to the model. Chapter 2 explained that Security was excluded since it was assumed to be relevant and being stringently applied. However, the Delphi Group made multiple points as to why it should be included. They stated that it directs how the other principles are allowed to be implemented and has an information focus. Therefore, Security was added to the model.

Security was also brought up as a barrier. There were several barriers commented on. The other barriers all could be linked to Culture in the sense that these barriers are a result of a set way of doing things. The change process was noted as inadequate and there is no legal reason it could not be modified, but cultural behavior dictates that since it has been established, it must be the right way. The MDA technically focused culture has established a modus operandi of enacting whatever new technology provides a specific capability. This conflicts with maintaining stable standards, but the cultural behavior is to favor technology rather than weigh the impact to the entire system. The tendency of forming stovepiped programs that leads to protectionist behavior is a cultural mindset. The lack of an obligatory sense to enact these principles on their own is a cultural manifestation of the military culture where directives are flowed down and self initiative is only rewarded if the benefits are immediately recognizable. Finally, the history of defense acquisitions has established the current cultural climate where contractors and government operate with hidden agendas that don't compliment one another. It is not surprising these barriers were mentioned and are linked to culture since the Delphi Group admitted culture is poorly understood.

Conclusions

The research question was answered and thesis supported by the Delphi Group that IM principles can be applied to the BMDS. The Delphi Group sited how culture plays a role in contractor selection, design, and manning. They also stated that without Information Strategy and IA they are constrained to optimization rather than creating what is truly needed by the system. Standards were identified as important as long as they were understood and consistent. Additionally, these principles, within the framework of a model, can aid the issue of integration. Information Strategy was called out as needed for determining information flow. The Delphi Group said an IA could help communication horizontally and vertically. The model should be considered for application across the entire BMDS: weapon systems, organization, acquisition, and processes. This includes application within the elements and between the elements as well, as the Delphi Group suggested. In addition to supporting the thesis, the process of writing this paper also strongly supported that DoD organizations involved with the BMDS are technically focused viewing technology as a solution, not an enabler. While the model should be considered for implementation, doing so would likely encounter serious cultural barriers such as those mentioned above which must be well understood.

Limitations of Research

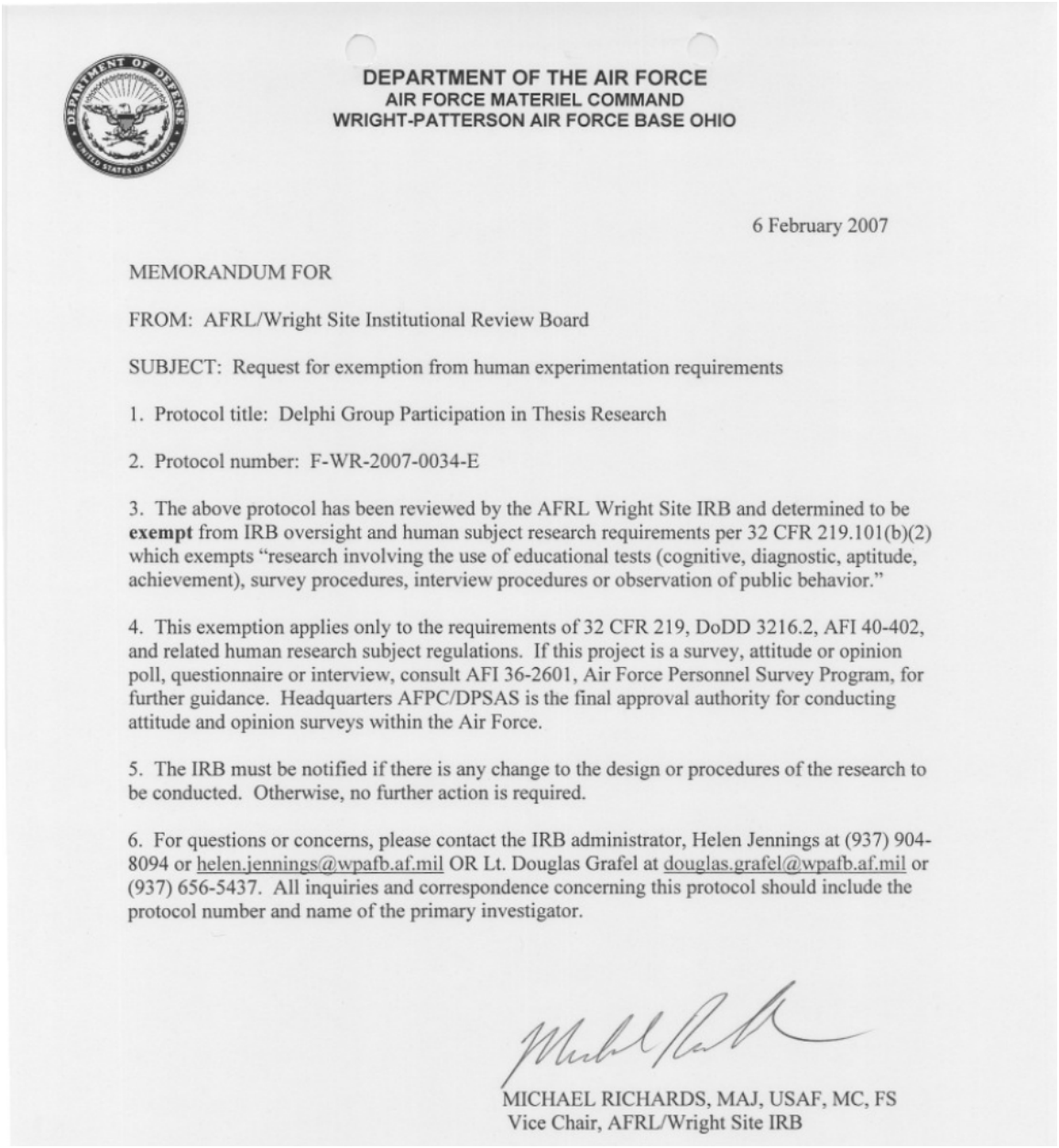
The Delphi Group was a panel of experts, but small in number. They also only had experience in some of the BMDS elements. While the Delphi Group had civilian

contractor experience, none were presently employees of civilian contractors. Finally, while relevant experts supported the model, it was not actually applied producing results that demonstrate its effects.

Recommendations for Future Study

Future studies should assemble a larger group with experience in various disciplines. Future study would benefit from a group representing each element, MDA, and USSTRATCOM. Future studies may benefit from the perspectives of employees of companies such as Boeing, LM, NG, and Raytheon who are all major contractors for multiple BMDS systems. Finally, future studies may benefit from undertaking an exercise where the model is applied and results are produced to measure its effectiveness. For example, it may be beneficial to apply the model to the GMD element which is composed of BMDS representative components. While it is expected that results would show limited effectiveness from being applied to a single element, this would confirm the need to apply the model across the entire system. Additionally, the necessary interconnects between elements may be identified.

Appendix A: Human Subjects Exemption Approval Letter



DEPARTMENT OF THE AIR FORCE
AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

6 February 2007

MEMORANDUM FOR

FROM: AFRL/Wright Site Institutional Review Board

SUBJECT: Request for exemption from human experimentation requirements

1. Protocol title: Delphi Group Participation in Thesis Research

2. Protocol number: F-WR-2007-0034-E

3. The above protocol has been reviewed by the AFRL Wright Site IRB and determined to be **exempt** from IRB oversight and human subject research requirements per 32 CFR 219.101(b)(2) which exempts "research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior."

4. This exemption applies only to the requirements of 32 CFR 219, DoDD 3216.2, AFI 40-402, and related human research subject regulations. If this project is a survey, attitude or opinion poll, questionnaire or interview, consult AFI 36-2601, Air Force Personnel Survey Program, for further guidance. Headquarters AFPC/DPSAS is the final approval authority for conducting attitude and opinion surveys within the Air Force.

5. The IRB must be notified if there is any change to the design or procedures of the research to be conducted. Otherwise, no further action is required.

6. For questions or concerns, please contact the IRB administrator, Helen Jennings at (937) 904-8094 or helen.jennings@wpafb.af.mil OR Lt. Douglas Grafel at douglas.grafel@wpafb.af.mil or (937) 656-5437. All inquiries and correspondence concerning this protocol should include the protocol number and name of the primary investigator.

MICHAEL RICHARDS, MAJ, USAF, MC, FS
Vice Chair, AFRL/Wright Site IRB

Bibliography

Auster, E., & Wei Choo, C. (1996). "Managing information for the competitive edge." New York: Neal-Schuman Publishers, Inc.

BMDS booklet: A day in the life of the BMDS (2006). (3rd ed.). Washington DC: Missile Defense Agency. Retrieved July 15, 2006, from http://www.mda.mil/mdalink/pdf/bmdsbook.pdf

Brown, N. (2005). "Interception at sea: Opening a new chapter for BMD." *Jane's Defense Weekly*, July 15, 2005 . Retrieved July 15, 2005, from http://search.janes.com

Burkett, Daniel L., II. (1998). *SBIRS overview: System program office program description.* Retrieved July 15, 2006, from http://www.fas.org/spp/military/program/warning/sbirs-brochure/index.html

Crock, S. (2002, May 13, 2002). "Is this missile defense an eagle - or an albatross?" [Electronic version]. *Business Week*, Retrieved July 15, 2006,

Department of energy - information architecture project: DOE corporate systems information architecture(2000). U.S. Department of Energy. Retrieved November 15, 2006, from http://cio.energy.gov/CSIA_Final.pdf

Department of the Navy, Information Management and Information Technology Strategic Plan(2006). Strategic Plan. Washington DC: Department of the Navy. Retrieved 15 Nov 06, from www.doncio.navy.mil/fy06stratplan/

Evernden, R., & Evernden, E. (2003). *Information first: Integrating knowledge and information architecture for business advantage*. Amsterdam: Elsevier.

Galliers, R. D., & Leidner, D. E. (2003). *Strategic information management: Challenges and strategies in managing information systems* (3rd ed.). Oxford: Butterworth Heinemann.

General Accounting Office. (2006). *Defense acquisitions: Assessment of selected major weapon programs*. Washington DC: General Accounting Office. Retrieved July 15, 2006, from www.gao.gov

General Accounting Office. (2006). *Defense acquisitions: Missile defense agency fields initial capability but falls short of original goals* No. GAO-06-327). Washington DC: General Accounting Office. Retrieved July 15, 2006, from www.gao.gov

General Accounting Office. (1993). *Ballistic missile defense: Evolution and current issues* No. GAO/NSIAD-93-229). Washington DC: General Accounting Office. Retrieved July, 2006, from www.gao.gov

Gordon, J., & Gordon, S. (1999). *Information Systems: A Management Approach* . Fort Worth: Dryden Press Harcourt Brace College Publishers.

Ground-based mid-course defense (GMD) segment. (2005). *Jane's*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Hewish, M. (2004). "Ballistic Missile Defense Aims to Keep its Feet on the Ground." *Jane's Defense Weekly*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Hewish, M. (2002). "Back in the Melting Pot." *Jane's*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Information Management Principles. (2006). Retrieved November 15, 2006, from http://www.monash.edu.au/staff/information-management/principles/

Information Management Principles. (2006). Retrieved November 15, 2006, from http://ioc.unesco.org/Oceanteacher/OceanTeacher2/03_InfoMgtPrinc/InformationMgtPrinciples.htm

Jane's Information Group. (2005). "Ballistic missile defense." *Jane's*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Larsen, J. A., & Kartchner, K. M. (2004). "Emerging Missile Challenges and Improving Active Defenses" Analysis. Maxwell Air Force Base, Alabama: USAF Counterproliferation Center. Retrieved 15 July, 2006, from http://www.au.af.mil/au/awc/awcgate/awc-cps.htm

Laudon, K. C., & Laudon, J. P. (1997). *Essentials of Management Information Systems: Organization and Technology* (2nd ed.). New Jersey: Prentice Hall.

Linstone, H. A., & Turoff, M. (1975). *The Delphi Method: Techniques and Applications*. Retrieved 26 February 2007, from http://is.njit.edu/pubs/delphibook/

"Lockheed Martin Missiles and Fire Control Patriot Advanced Capability-3 (PAC-3) Missile." (2006). *Jane's*, September 15, 2006 from http://search.janes.com

Lorell, M. A., & Grasser, J. C. (2000). *RAND Monograph Report: An Overview of Acquisition Reform Cost Savings Estimates* (Informational No. MR1329) RAND. Retrieved July 15, 2006, from http://www.rand.org/pubs/monograph_reports/MR1329/MR1329.ch3.pdf

MDA Historian Office. (2001). *Ballistic Missile Defense: A Brief History*. Retrieved July/16, 2006, from http://www.mda.mil/mdalink/html/briefhis.html

Robertson, J. (2005). "10 Principles of Effective Information Management." *KM Column*, July 15, 2006 . Retrieved July 15, 2006, from www.steptwo.com.au

Singer, J. (2005). "Pentagon Scales Back SBIRS Program." Retrieved 20 November, 2006, from http://www.space.com/spacenews/archive05/Sbirs_121905.html

Sirak, M. (2004). "Ballistic Missile Defense: The End Game." *Jane's Defense Weekly*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Sirak, M. (2001). "Lt Gen Ronald Kadish - Director of the US Ballistic Missile Defense Organization." *Jane's Defense Weekly*, July 15, 2006 . Retrieved July 15, 2006, from http://search.janes.com

Wigand, R., Picot, A., & Reichwald, R. (1997). *Information, Organization and Management: Expanding Markets and Corporate Boundaries*. Chichester: John Wiley & Sons.

Wilson, D. A. (1993). *Managing Information*. Oxford: Butterworth Heinemann.

Vita

Captain John M. Koehler II graduated from Santa Monica High School in Santa Monica, California. He entered undergraduate studies at the Loyola Marymount University in Los Angeles, California where he graduated with a Bachelor of Science degree in Mechanical Engineering in December 1998. He was commissioned through Detachment 55/A AFROTC at Loyola Marymount University where he was recognized as a Distinguished Graduate.

His first assignment was at Vandenberg AFB as a student in Undergraduate Space and Missile Training and Peacekeeper ICBM Initial Qualification Training in February 1999. In September 1999, he was assigned to the 400th Missile Squadron, F. E. Warren AFB, Wyoming where he served as a missile operations officer. He next served as a developmental engineer at the Space and Missiles System Center, Los Angeles AFB for the Space Tracking and Surveillance System Special Projects Office from November 2003 to August 2005. In September 2005, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to Detachment 1, 2nd Space Warning Squadron, Schreiver AFB where he will operate the Space Based Infrared System.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**			
1. REPORT DATE *(DD-MM-YYYY)* 22-03-2007	**2. REPORT TYPE** **Master's Thesis**		**3. DATES COVERED** *(From – To)* Aug 2005 – Mar 2007
4. TITLE AND SUBTITLE Information Management Principles Applied to the Ballistic Missile Defense System			**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Koehler, John M., Captain, USAF			**5d. PROJECT NUMBER** If funded, enter ENR # **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765			**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GSS/ENV/07-M2
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Col Christopher E. Pelc Space Tracking and Surveillance System Special Project Office 483 N. Aviation, Bldg 271 Rm B4-578 El Segundo, CA 90245 633-3319			**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.			
13. SUPPLEMENTARY NOTES			
14. ABSTRACT Information systems (IS) have evolved over the last 50 plus years from individual components with single functionality to grand architectures that integrate multiple individual business functions into global organizational enterprises. Similarly several military systems with the single mission of missile defense have evolved in service stovepipes, and are now being integrated into a national and global missile defense architecture. The Missile Defense Agency (MDA) is currently tasked with developing an integrated Ballistic Missile Defense System (BMDS) capable of defending against all ranges of ballistic missiles in all phases of flight in defense of the homeland, our deployed forces, and our allies. While this initiative has been proceeding since before Ronald Reagan's Strategic Defense Initiative, the full momentum has only recently been achieved through the withdrawal of the Anti-Ballistic Missile Treaty and demonstrated threats from North Korea and Iran. This study draws parallels between the evolution of IS and the BMDS. Further it compiles information management (IM) principles, investigates if they apply to the BMDS, and investigates if they can be used to achieve a better integrated system. Initial indications are that IM principles do apply, but it is questionable if they are being applied.			
15. SUBJECT TERMS Information Management, Delphi Technique, Principles, Ballistic Missile Defense			

16. SECURITY CLASSIFICATION OF: Unclassified			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Alan R. Heminger PhD (ENV)
REPORT U	**ABSTRACT** U	**c. THIS PAGE** U	UU	77	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 7405; e-mail: Alan.Heminger@afit.edu

Standard Form 298 (Rev: 8-98)
Prescribed by ANSI Std. Z39-18